



June 14, 2010

Office of the Secretary;
National Telecommunications and
Information Administration;
International Trade Administration
US Department of Commerce
1401 Constitution Avenue, N.W.
Room 4725
Washington, D.C. 20230

Filed by email at privacy-noi-2010@ntia.doc.gov

Re: Department of Commerce Notice of Inquiry
Information Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01; RIN 0660-XA12

The Council of Better Business Bureaus (CBBB) appreciates the opportunity to provide these comments in response to the US Department of Commerce's ("the Department") "Notice of Inquiry on Information Privacy and Innovation in the Internet Economy," 75 FR 21226, issued April 23, 2010.

The NOI seeks comments on the efficacy of current privacy laws and self regulatory initiatives in the United States and worldwide in supporting internet commerce and innovation, while maintaining fundamental privacy principles and taking account of evolving consumer expectations regarding online privacy. These issues were explored during panel discussions at the Department's related Symposium on Privacy and Innovation held May 7, 2010, in which CBBB was pleased to participate.

We applaud the Department's initiative in launching this fact finding effort, and in providing a forum for dialogue around approaches to privacy accountability that

Council of Better Business Bureaus, Inc.

4200 Wilson Boulevard, Suite 800 • Arlington, Virginia 22203 • Phone: 703.276.0100 • Fax:
703.525.8277

foster continued innovation across the internet ecosystem, while respecting and protecting consumer privacy

We note two recurring themes that emerged during the Symposium. First, in the global internet economy, privacy accountability for the collection, transfer and use of personal data does not simply implicate individual rights within one jurisdiction, but also affects the flow of international trade. Many individual privacy complaints arising from online commerce cannot be readily handled in the cross border environment, where varying legal privacy frameworks may provide few traditional options for resolution of consumer disputes. Even in countries with well-developed privacy rules, regulatory intervention is unlikely to occur until a critical mass of complaints has been received against a single perpetrator, and the vast majority of consumer privacy disputes are unlikely to be adjudicated within traditional judicial systems, given the barriers of expense, language, access and procedural complexities and the low monetary value of most disputes.

In our comments we will reference CBBB's experience and belief that these issues may be addressed most effectively and economically by flexible self-regulatory frameworks for handling complaints and adjudicating privacy disputes against mutually agreed principles. A key element of such frameworks is the inclusion of independent third party accountability mechanisms to support and enforce industry compliance and to resolve consumer privacy disputes that might otherwise go unaddressed.

Our comments will also touch on a second theme of the Symposium – how the evolving privacy expectations of internet users regarding the passive collection and use of their personal data in certain contexts have exposed the limitations of traditional notice and choice in the privacy policy. CBBB recognizes the need for innovative approaches to consumer awareness and participation in authorizing the collection, transfer and use of personal data and other unique identifiers in contexts such as online marketing. To this end, CBBB has participated in the development of the first cross-industry Self-Regulatory Principles for Online Behavioral Advertising, released in July 2009 and discussed below.

I. CBBB Background

The Council of Better Business Bureaus, a non-profit 501(c) (6) membership organization, is the umbrella organization for local Better Business Bureaus, which are grassroots organizations that foster a fair and honest marketplace and an ethical business environment. The mission of the BBB system is to advance marketplace trust by promoting the highest ethical relationship between businesses and the public through self-regulation, consumer and business education, and service excellence.

The CBBB has administered self regulatory programs in the advertising industry for almost 40 years, and has created innovative compliance and dispute resolution programs to address other emerging issues, including the highly regarded *BBB AUTOLINE* and *BBB Online* programs. The CBBB also has demonstrated leadership in online advertising and privacy issues. Its *Children's Advertising Review Unit (CARU)* administers the first FTC-granted safe harbor under the Children's Online Privacy Protection Act. The CBBB developed one of the earliest online privacy seal programs, and its *BBB EU Safe Harbor* program remains a prominent dispute resolution mechanism under the US-EU Safe Harbor Framework. Most recently, CBBB and a coalition of advertising industry associations spearheaded the development and release in July 2009 of the *Self Regulatory Principles for Online Behavioral Advertising*.

II. Self Regulation and International Privacy Frameworks

A. Key Concepts in Self Regulation

While business self-regulation is well recognized in the United States, it is less understood in other parts of the world. CBBB has long argued that the term "self" in self-regulation should not be understood as industry acting unilaterally, but rather as a process driven by the enlightened self-interest of industry, supported in limited, but critical, ways by government to the ultimate benefit of consumers. The Better Business Bureau system has many years of highly successful experience with self-regulation in the U.S. and Canada. Based on that experience, we believe that successful self-regulatory frameworks include performance and voluntary compliance standards that are developed by industry, recognized and complemented by objective third party oversight, and credible to the public.

Any self-regulatory process that lacks substance or fails to deal firmly and openly with conduct at variance with the voluntary guidelines will lose the confidence of both consumers and regulators, resulting in often sweeping regulation that can strangle innovation and discourage competition.

Industry can play a pivotal role in developing international self-regulatory privacy frameworks by encouraging the development of standards for online commerce, and funding the development of the technology infrastructure needed to ensure dispute resolution mechanisms are both cost-effective and provided at low or no cost to consumers. It can develop private sector funding to support independent “accountability agents” such as trustmark organizations and other third party monitoring mechanisms. It can also encourage effective partnering across borders among consumer groups, dispute resolution programs and self-regulatory organizations.

National governments can play an equally vital role by adopting cross border principles that complement and encourage the development of national privacy laws; establishing standards for accountability agents and dispute resolution mechanisms; and taking action under national laws and regulations when certified companies fail to honor their commitments under international frameworks. The CBBB believes that self-regulatory frameworks meeting these criteria provide the best model for consumer privacy protection in the global e-commerce environment.

Two international initiatives spearheaded by the Department of Commerce incorporate these self-regulatory elements: the US-EU Safe Harbor Privacy Framework, now in its tenth year of operation; and the APEC Privacy Pathfinder Projects, dedicated to developing a Cross Border Privacy Rules system for cross border data transfers across the APEC economies.

B. US-EU Safe Harbor Privacy Framework

After a decade in operation, the US-EU Privacy Framework has seen a rapid expansion in participation over the last two years by US companies doing business in the European Union, who choose to self-certify their compliance with the Safe Harbor Principles as a mechanism to facilitate transfers of personal data from the European

Union member states. We understand that around 2,000 companies are registered on the Department's Safe Harbor List, with up to 50 new companies filing initial self-certifications each month.¹

Alternative data transfer mechanisms are available, including Model Contracts pre-approved by the European Commission for transfers to both the US and other destinations, and Binding Corporate Rules, enabling affiliated companies operating in multiple jurisdictions to obtain approval from the DPAs to use internal privacy rules based on EU data privacy principles for cross border data flows within affiliate groups. However, for most US businesses, and particularly for smaller concerns doing business online with non-affiliated entities in the EU, the Safe Harbor Framework appears to offer a more practical, less burdensome option.

Equally importantly, participation in the Safe Harbor Framework creates a level of public accountability for US companies within the United States. Participants must self-certify to the Commerce Department and in published privacy statements that their privacy practices conform to the seven Safe Harbor Privacy Principles, and must verify that compliance during annual recertification. Verification may be performed in-house and certified by senior management, or may be provided by a commercial seal program or other independent verifier. Participating companies also are required to designate an affordable, accessible independent dispute resolution mechanism to handle complaints by EU data subjects. In addition, the Federal Trade Commission ("FTC") has enforcement authority over both the Framework participants and over commercial trustmarks who may verify their compliance.

We note two developments in 2009 that will likely bolster the Framework's effectiveness: the FTC's first two enforcement actions against a total of seven companies that had falsely represented their self-certification to the Safe Harbor Program in their online privacy statements (one had never certified; six others had allowed their certifications to lapse); and the imposition of certification fees for participation, providing the Department of Commerce with additional resources to keep the Safe Harbor List of certified participants updated and accurate. These actions can be expected to refocus participating companies on the substantive

¹ See Brian Hengesbaugh, Michael Mensik, Amy de La Lama, *Why Are More Companies Joining the US-EU Safe Harbor Framework?* IAPP Privacy Advisor, Vol. 10, No. 1 (January –February 2010).

commitments they have made to privacy protection, and to increase public confidence in the efficacy of the Framework.

C. The APEC CBPR System

We wish to commend the Department for its continuing leadership in the APEC Data Pathfinder Projects, which seek to bring together all stakeholders – governments, regulators, industry, consumer representatives and accountability agents – in a consultative process to create and test the elements of the cross border privacy rules (CBPR) system to enable cross border data flows across the APEC economies under the guidance of the APEC Privacy Principles. The system is intended to provide a mechanism for certification by accredited accountability agents of a business's internal 'privacy rules' as compliant with the Principles. Such certifications are to have mutual recognition among participating economies. The system is also expected to guarantee backstop enforcement by a public sector enforcement authority with jurisdiction to enforce domestic privacy laws. The CBPR system is intended to promote a minimum standard of privacy protection for data transfers across participating economies, while maintaining the obligations of participating companies to comply with all applicable domestic laws.

Given that the proposed CPBR certification system will subject the business processes and privacy practices of participating companies to an intensive process of self-assessment and external review, the qualifications and roles of accountability agents have received well deserved scrutiny. At present, the proposed system provides some flexibility as to which entities may perform the accountability tasks of certifying businesses, monitoring compliance, dispute resolution and enforcement. Certain private sector accountability agents – including established trustmark or seal programs – may assert their ability to play all of these roles. Other entities that are well qualified to evaluate and certify privacy compliance, such as law or accounting firms or public sector agencies, may be unable to demonstrate sufficient 'independence' in their relationships with certified businesses to also offer dispute resolution services. Such entities may elect to provide only certification and limited compliance monitoring, while partnering with qualified entities to provide independent dispute resolution and enforcement. As discussions progress, we expect that the eligibility standards for accountability agents – including, but not limited to, independence and freedom from conflicts of interest – will be critical to maintaining

the confidence of businesses, consumers and governments in the ability of the CBPR system to protect consumer privacy while maintaining information flows across the APEC economies and preserving the vitality of internet commerce.

III. Self-Regulation of Online Behavioral Advertising (OBA)

In July 2009, following months of collaborative efforts by associations and individual companies representing the entire online advertising ecosystem, a coalition of trade associations including the CBBB, together with the Association of National Advertisers, the American Association of Advertising Agencies, the Interactive Advertising Bureau, and Direct Marketing Association released the cross-sector *Self-Regulatory Principles for Online Behavioral Advertising*², the first self regulatory framework designed to apply broadly to all of the actors engaged in online behavioral advertising activities. The seven Principles include commitments to consumer education; new consumer notice and choice mechanisms; data security; increased protection for sensitive data categories such as medical and financial information and children's data; affirmative consent for material changes to online behavioral advertising data collection and use policies; and strong enforcement mechanisms.⁶

A. Transparency and Choice

Key elements of the Principles provide both for more transparent notice of how consumer data is collected and used and for simple and effective processes for consumers to choose whether to receive behaviorally targeted ads. Companies engaged in behavioral advertising are directed to explain their activities on the relevant websites outside the privacy policy, by placing a consistent icon and common notice language in proximity to behaviorally targeted online ads or in another prominent location on web pages where behavioral data is collected. Web site operators hosting behavioral advertising, as well as the third party ad networks, behavioral data providers and others collecting behavioral data or serving ads on their sites are called on to provide links from this enhanced notice to consumer preference pages or choice mechanisms. In addition to these innovative solutions, the Principles include specific commitments to provide consumer education on

² American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau, and Council of Better Business Bureaus, *Self-Regulatory Principles for Online Behavioral Advertising* (July 2009), available at <http://www.bbb.org/us/behavioral-advertising-principles/>

behavioral advertising practices and on the significance and functionality of the icon and the enhanced notice and choice mechanisms. They also call for the creation of accountability mechanisms – now under development by CBBB and by the Direct Marketing Association –that will police and enforce industry compliance with the Principles, handle consumer complaints, help bring entities into compliance, publicly report instances of noncompliance, and refer persistent violators to the appropriate government agencies.

B. Accountability

The CBBB believes that a robust and independent accountability mechanism is critical to the success of self-regulatory programs. Accordingly, with support from the industry Coalition, the CBBB is currently developing an accountability mechanism to monitor compliance with the OBA Principles, to be modeled loosely on the highly successful Children’s Advertising Review Unit or CARU, a CBBB-administered program whose operational policies are set by the National Advertising Review Council (NARC).³ Like CARU, CBBB’s OBA accountability mechanism will engage in widespread monitoring of web sites and companies known or believed likely to be engaged in behavioral advertising activities. To facilitate consumer complaint handling and to avoid duplication of effort, CBBB will coordinate its activities with those of the DMA, whose own accountability mechanism will ensure its members’ compliance with the Principles as implemented in the DMA’s Code of Ethical Guidelines.

IV. Conclusion

CBBB is proud of the progress that self-regulation has made toward protecting consumers while maintaining the dynamic, innovative environment of the internet, and we look forward to continuing our participation in both domestic and international self regulatory privacy programs. CBBB believes that sustained efforts by all interested groups to build alliances and relationships remain essential to the goal of fostering global online commerce to the benefit of consumers and merchants in every country.

³ NARC is a strategic alliance of the advertising industry and the BBB.

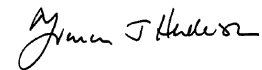
* * *

The CBBB thanks the Department of Commerce for the opportunity to submit these comments, and we look forward to working with the Department as it continues to evaluate the important issue of online privacy in the global internet economy.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "C. Lee Peeler".

C. Lee Peeler
Executive Vice-President
Council of Better Business
Bureaus

A handwritten signature in black ink, appearing to read "Frances J. Henderson".

Frances J. Henderson
Associate General Counsel
and Director, Privacy
Initiatives
Council of Better Business
Bureaus